HAFETZ NECHELES & ROCCO
ATTORNEYS AT LAW

500 FIFTH AVENUE
NEW YORK, N.Y. 10110
TELEPHONE: (212) 997-7595
TELECOPIER: (212) 997-7646
E-MAIL: INFO@HNRLAWOFFICES.COM

August 2, 2012

VIA ECF

The Hon. Steven M. Gold
Chief United States Magistrate Judge
United States District Court
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: *United States v. Lebovits, et al.*, No. 11 Crim. 134 (SJ-SMG)

Dear Chief Magistrate Judge Gold:

We submit this letter to address two issues which arose at oral argument on July 19: (1) whether suppression of Moses Neuman's wiretapped conversations and the emails seized from his emails accounts is required due to the government's flagrant disregard of Mr. Neuman's rights, and (2) whether AUSA Kleinberg's assertion at oral argument that Judge Johnson had already decided this issue was a factually incorrect statement.

I. Suppression Is Required

A. Facts

In the course of its investigation, the government obtained orders to wiretap Mr. Neuman's phone. The facts surrounding the wiretap applications are set forth on pages 5–17 of Mr. Neuman's initial brief, Docket No. 66, and the facts concerning the government's "minimization" by actually taping the Yiddish calls and subsequently reviewing them are set forth on pages 27–28 of that brief.

Additionally, the government obtained search warrants entitling it to seize relevant emails from Mr. Neuman's email accounts. The warrants specifically required that (1) the email providers would provide all of Mr. Neuman's emails to a government taint team, (2) the taint team would search the emails to determine which emails the government were within the scope

of the search warrant and the government was accordingly entitled to seize, and (3) the taint team would then produce to the investigative agents and prosecution team only those emails within the scope of the warrant.

The government then produced to all of Mr. Neuman's co-defendants the supposedly "minimized" tapes and the emails it was not entitled to seize. On May 11, 2011, the government produced Rule 16 discovery to the defendants. This discovery included (1) a small amount of scanned paper documents, including the emails identified by the taint team as within the scope of the warrant and shared with the prosecution team, which were sent directly by the government to each defendant in the case, and (2) electronic files on CDs, which was the bulk of the discovery. Among the electronic files which were provided to all defendants were (a) the full sets of Moses Neuman's emails produced by the email providers to the taint agents, including the emails which the government was *not* entitled to seize, and (b) *all* wire communications intercepted on Moses Neuman's phone pursuant to the wiretap orders, including personal and non-pertinent conversations recorded by the government which purportedly were "minimized" but actually were recorded. Unlike the scanned paper documents, the CDs containing the electronic files were not sent by the government directly to the defendants. Rather, the government instructed that the defendants were to obtain copies of the electronic files via a government vendor.

Thus, on the afternoon of May 11, AUSA Charles Kleinberg telephoned Moses Neuman's defense counsel Joshua Geller and informed him that the government was making available to all defendants a production of electronic documents via government vendor First Choice Copy. Mr. Geller arranged with counsel for the co-defendants that Hafetz Necheles & Rocco would obtain one copy of the discovery from First Choice and, because First Choice was charging more than double what other copy services would charge, would send the discs to another copy service to make copies for each defendant, and the defendants would share equally in the copying costs. Over the next few days this is what occurred and by May 16, all defendants had in their possession a full set of the CDs that Mr. Kleinberg had told defense counsel were available for all defendants at First Choice Copy.

Also on May 11, Mr. Kleinberg mailed to defense counsel a multi-page letter that purported to index the voluminous documents in the 22 CDs provided to defense counsel. This letter reaffirmed what Mr. Kleinberg had said on the phone – all 22 CDs were being made available to all defendants. Defense counsel did not attempt to parse through the details of what had been produced that were contained in this dense letter, but instead set the letter aside for a later date, to use as an index when reviewing the discovery.

More than one month after the production, on June 28, 2011, the government sent a letter to all defendants in the case admitting that it had wrongfully produced Moses Neuman's privileged and non-pertinent calls to all the defendants in the case:

The government, under cover of its May 11, 2011 discovery letter (the "May 11 Letter"),

> mistakenly made Disks 44 and 45, including the privileged and non-pertinent calls contained thereon, available to all of the defendants, instead of making the Neuman privileged and non-pertinent calls available only to Moses Neuman . . . .

Government June 28 Letter at 3.

Even after realizing that it wrongfully disseminated the calls and emails, the government did nothing to cure its error. The government did not seek an order from this Court requiring the co-defendants to return the wrongfully distributed Title III materials to the government. Nor did the government even inform the Court of what had occurred. Rather, the government simply proposed in its June 28 letter and a subsequent letter dated July 14 that the co-defendants return to the government Mr. Neuman's privileged and non-pertinent calls.

Furthermore, the government did not check to ascertain whether it had also wrongfully made available other materials to the co-defendants in addition to the privileged and non-pertinent calls. In fact, the government had also made available to the co-defendants via the March 11 production copies of Mr. Neuman's privileged and non-pertinent emails that the government was not authorized to seize.

Among the "minimized" recorded calls and the non-pertinent emails that the government made available to the co-defendants are incredibly private and intimate communications of Mr. Neuman, including conversations between Mr. Neuman and his wife, his father, his rabbi, and his wife's doctor. In a sealed *ex parte* declaration accompanying this letter, we attach or describe some of these emails and calls so that that Court can understand the magnitude of the harm to Mr. Neuman as a result of their dissemination. Due to the government's wrongful conduct, these emails and calls were in the co-defendants' possession from May 2011 through September 2011, when Judge Johnson issued a protective order directing that the co-defendants send the material to the Court for placement under seal. We know that, during this five-month period, at least one of the co-defendants reviewed all of the calls and emails, including the highly sensitive communications described in the *ex parte* declaration.

B. The Suppression Of Moses Neuman's Wiretapped Conversations Is Required By Title III and the Constitution

1. *The Wiretaps Must Be Suppressed Due To The Government's Violation Of Title III*

Title III authorizes disclosure of wiretaps only to the extent that such disclosure "is appropriate to the proper performance of [law enforcement] official duties." 18 U.S.C. § 2517(2). Title III does *not* authorize disclosure of minimized conversations to anyone other than the person whose conversations were taped.

In *United States v. Giordano*, 416 U.S. 505 (1974), the Supreme Court explained what kinds of Title III violations merit suppression under its suppression provision, 18 U.S.C. § 2518(10)(a)(i). The Court noted that when the government ignores a statutory requirement that "was intended to play a central role" in Title III, "suppression must follow." *Id.* at 528; *see also United States v. Chavez*, 416 U.S. 562, 578 (1974) (suppression appropriate for violation of statutory provision that plays "a central, or even functional, role in guarding against unwarranted use of wiretapping or electronic surveillance"); *United States v. Marion*, 535 F.2d 697, 701 n.7 (2d Cir. 1976) (noting that Title III provides for suppression where communications were "unlawfully intercepted" and "[t]he words 'unlawfully intercepted' are themselves not limited to constitutional violations,' but include a failure to satisfy requirements of Title III as well") (*quoting Giordano*, 416 U.S. at 527).

Clearly, the disclosure provisions of Title III play a "central" and "functional" role in balancing the competing privacy and law enforcement interests at the heart of Title III. Indeed, the procedures governing disclosure in Title III play as important a role as the procedures governing interception. As the Second Circuit acknowledged in *SEC v. Rajaratnam*, 622 F.3d 159 (2d Cir. 2010), "there is a distinct privacy right against the *disclosure* of wiretapped private communications that is separate and apart from the privacy right against the *interception* of such communications . . . ." *Id.* at 169 (emphasis in original). This was also made clear by Judge Gleeson's analysis of Title III in *United States v. Simels*, No. 08-CR-640, 2009 WL 1924746 (E.D.N.Y. July 2, 2009). Judge Gleeson explained in *Simels* that Title III's legislative history makes clear that Congress intended not only to ensure the minimization of the interception of non-pertinent communications, but also to restrict the dissemination of non-pertinent communications. *Id.* at *4.

Here, in wrongfully making available to the co-defendants the recordings of Mr. Neuman's privileged and non-pertinent calls, the government violated Title III's disclosure provision. Pursuant to *United States v. Giordano*, the government's blatant violations of Title III's disclosure requirements mandate suppression.[1]

2. *The Wiretaps Must Be Suppressed Due To The Government's Flagrant Disregard Of Mr. Neuman's Constitutional Rights*

Suppression of the wiretaps is separately required because the wrongful disclosures of the privileged and non-pertinent calls that occurred here violated Mr. Neuman's constitutional right to privacy. As the Supreme Court pointed out in *Bartnicki v. Vopper*, 532 U.S. 514 (2001):

[1] By making the privileged and non-pertinent calls available to the co-defendants, the government also violated Judge Townes's April 11, 2011 unsealing order, which provided that the wiretapped calls were to be unsealed "solely for the purpose of making discovery" in this case. Plainly, Federal Rule of Criminal Procedure 16(a)(1)(E), which requires the government to disclose evidence that is material to preparing the defense or that the government intends to use at trial, did not require the government to disclose the privileged and non-pertinent calls to the co-defendants.

> [T]he disclosure of the contents of a private conversation *can be an even greater intrusion on privacy than the interception itself.* As a result, there is a valid independent justification for prohibiting such disclosures by persons who lawfully obtained access to the contents of an illegally intercepted message, even if that prohibition does not play a significant role in preventing such interceptions from occurring in the first place.

Id. at 533 (emphasis added); *see also Gelbard v. United States*, 408 U.S. 41, 51–52 (1972) ("[c]ontrary to the Government's assertion that the invasion of privacy is over and done with, to compel the testimony of [ ] witnesses compounds the statutorily proscribed invasion of their privacy by adding to the injury of the interception the insult of compelled disclosure"); *Fultz v. Gilliam*, 942 F.2d 396, 402 (6th Cir. 1991) ("[e]ach time the illicitly obtained recording is replayed to a new and different listener, the scope of the invasion widens and the aggrieved party's injury is aggravated").

These principles informed the Second Circuit's conclusion in *Rajaratnam* that "there is a distinct privacy right against the *disclosure* of wiretapped private communications that is separate and apart from the privacy right against the *interception* of such communications." *Rajaratnam*, 633 F.3d at 169. In effect, improper disclosure of wiretap communications, even if they had been properly seized – and it is Mr. Neuman's position that the government failed to properly minimize his privileged and non-pertinent calls – is another "search" under the Fourth Amendment – invading an individual's private space, and exposing his most personal moments to public glare. The appropriate remedy for this is suppression. *See, e.g., United States v. Amanuel*, 615 F.3d 117, 127 (2d Cir. 2010) ("blanket suppression of the intercepted communications and all evidence derived therefrom" may be appropriate in the context of constitutional violations).

Here, it is beyond dispute that Mr. Neuman's privacy rights were violated by the improper disclosures that occurred here: private – and in many cases intensely personal – calls that have absolutely no bearing on the facts of this case were turned over to Mr. Neuman's co-defendants, who had access to the tapes until the Court issued a protective order. The improper disclosure of these privileged and non-pertinent calls is of constitutional magnitude because it constituted a staggering invasion of Mr. Neuman's privacy. *See Rajaratnam*, 633 F.3d at 170 (when improperly disclosed wiretap recordings are "listened to, . . . the privacy rights of the parties to the conversations will forever have been harmed by the very act of exposure"). It is clear that Mr. Neuman's constitutional right to privacy has been irreparably violated by the disclosure of his non-pertinent and private communications to the co-defendants, and the only meaningful remedy is suppression. *See United States v. Renzi*, 722 F.Supp.2d 1100, 1128 (D. Ariz. 2010) (suppressing entire wire where government not only wrongfully intercepted attorney-client privileged communications in violation of the Fourth Amendment, but compounded this harm by "the distribution of privileged calls to [the interceptee's] codefendants"). *See also*

Simels, 2009 WL 1924746, at *9 (suppressing entire wire where government acted unreasonably by recording privileged attorney-client communications in violation of Title III's minimization requirement).

3. *Moses Neuman's Emails Must Be Suppressed Due To The Government's Flagrant Disregard Of The Search Warrants*

Blanket suppression of evidence obtained pursuant to a search warrant is required when the government agents "flagrantly disregard" the terms of the warrant by effecting a widespread seizure of items that were not within the scope of the warrant and failing to act in good faith. *United States v. Liu*, 239 F.3d 138, 140 (2d Cir. 2000). Here, the government's outrageous conduct in making available to the co-defendants Mr. Neuman's privileged and non-pertinent emails meets the *Liu* blanket suppression standard and the emails must be suppressed.

The process set out in the search warrants providing that a taint team would review the emails and provide to the prosecution team only those emails relevant to the investigation was crucial to the warrants' constitutionality. The government may not seize electronic data without regard to whether it falls within the scope of a search warrant. *See United States v. Vilar*, No. S-305-CR-621-KMK, 2007 WL 1075041, *36 (S.D.N.Y. April 4, 2007) ("when the government seeks to seize the information stored on a computer . . . that underlying information must be identified with particularity and its seizure independently supported by probable cause"). To seize indiscriminately all of the electronic data would be a general search and seizure, a fundamental violation of the Fourth Amendment. *See id.* at *35 (noting that "searches of computers raise unique Fourth Amendment issues" because "[c]omputers . . . often contain significant 'intermingling' of relevant documents with 'documents that the government has no probable cause to seize.'). Even where a warrant allows the government to obtain from an email provider a copy of all emails in an email account, the government is not entitled to "seize" all the data it obtains. Instead, after searching the electronic data, the government may seize *only* those emails that fit within the parameters set by the search warrant. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring) ("The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.").

A very recent decision from this District establishes that the government's making available to the co-defendants Mr. Neuman's emails that fell outside the scope of the search warrants requires suppression under the *Liu* "flagrant disregard" standard. In *United States v. Metter*, No. 10-CR-600, 2012 WL 1744251 (E.D.N.Y. May 17, 2012), the government asserted that the defendant in a securities fraud action used his computer to further the alleged crime. After obtaining search warrants, the government seized the defendant's computer hard drives and the emails from his internet search providers. The government then stated that it intended to produce all of the seized electronic evidence to all of the defendants, without first conducting a

privilege review. *Id.* at *5. Defense counsel objected to this approach, stating at a status conference before the court:

> It is very troubling to me that the Government would take the position that they can come in and seize a computer with probably years' worth of confidential completely irrelevant material on it and then disseminate it out to a group of other individuals. This is completely apart from attorney-client privilege. This is really a matter of irrelevant personal confidential data. Heaven only knows what's on there. Financial data, personal information, relationship information. That cannot—that can't be permissible.

Id. at *5.

The *Metter* court suppressed all of the evidence on the basis that the government not only failed to timely review the evidence to determine whether it fell within the scope of the warrant, but also planned to release to the co-defendants the entire body of seized electronic data, not just those emails within the scope of the warrant. The court held that "the release to the co-defendants of any and all seized electronic data without a predetermination of its privilege, nature or relevance to the charged criminal conduct . . . compounds the assault on [the defendant's] privacy concerns. It underscores the government's utter disregard for and relinquishment of its duty to insure that its warrants are executed properly." *Id.* at 9.

The *Metter* court concluded that blanket suppression of the seized electronic evidence was appropriate because the government "flagrantly disregarded" the terms of the warrant by (1) effecting a "widespread seizure of items that were not within the scope of the warrant" and (2) not acting in good faith. *Id.* at *10 (*citing Liu*, 239 F.3d at 140). With respect to the first prong of the *Liu* test, the *Metter* court held that the search amounted to an unconstitutional general search in violation of the Fourth Amendment because the government effected a "widespread seizure of *all* information contained in the personal email accounts and computers at issue with imaging and review to occur off-site." *Id.* at *10. With respect to the second prong, the court held that the government's lack of good faith could be inferred by its conduct in failing to timely review the evidence and threatening to provide all of the seized evidence, including emails not within the scope of the search warrant, to the co-defendants. *Id.*

Here, as in *Metter*, the government's conduct meets both prongs of the "flagrant disregard" *Liu* test. First, the government's seizure of all of Mr. Neuman's emails and its plan to have a taint team review perform a subsequent off-site review of the emails for responsiveness to the warrant is indistinguishable from the facts which the *Metter* court found resembled a general search. *Metter* at *10. With respect to the second prong, the government's conduct here strongly evidences a lack of good faith. Unlike in *Metter*, where the government only threatened to make all of the emails available to the co-defendants, here the government actually did so via is May 11, 2011 discovery production. While the government now self-servingly claims that it was merely "mistaken" in making all of Mr. Neuman's emails available to the co-defendants, the

fact remains that – even after its taint team reviewed the emails and designated certain emails as privileged or non-pertinent – the government took no precautions whatsoever to prevent the dissemination of Mr. Neuman's personal emails which were plainly beyond the scope of the search warrants. Further, the government sought no relief from this Court concerning its wrongful distribution of the emails – indeed, it did not even notify this Court of the issue – until Mr. Neuman moved for a protective order.

The *Metter* court articulated a hypothetical scenario to illustrate the privacy concerns inherent in the government's seizure of an entire email account: "the seizure of a personal email account could, in addition to evidence responsive to a search warrant, yield personal communications between a cheating spouse and his or her paramour or communications between an individual and his or her family regarding an embarrassing medical condition. These hypothetical communications clearly fall outside the scope of the search warrants in this case (and arguably those in most criminal cases)." *Id.* at *6. In this case, due to the government's abysmal failure to safeguard Mr. Neuman's private communications, these hypothetical concerns were realized, with devastating consequences to Mr. Neuman. Among Mr. Neuman's emails that were wrongfully made available by the government to the co-defendants are private communications of an extremely intimate and embarrassing nature, as set forth in the accompanying sealed *ex parte* declaration.

As the *Metter* court stated, if this Court were to allow the government to use the seized electronic evidence when it has so flagrantly disregarded the limitations in the search warrants by making available to the co-defendants Mr. Neuman emails which were beyond the scope of the warrants, "the Fourth Amendment would lose all force and meaning in the digital age and citizens will have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination." *Id.* at *10.

II. Judge Johnson Did Not Decide This Issue

On August 26, 2011, Mr. Neuman moved for a protective order directing the government and the co-defendants to deliver to the Court to be placed under seal Mr. Neuman's privileged and non-pertinent calls and emails. Docket No. 52. The government cross-moved for a protective order, admitting that it had mistakenly failed to ensure that no defendant received in discovery the non-pertinent or privileged communications of other defendants and that it "bears responsibility for disclosing privileged and non-pertinent communications of one defendant to other defendants." Government Memorandum of Law, Docket No. 53, at 13.

Neither Mr. Neuman nor the government addressed in these motion papers whether the government's misconduct in making these privileged and non-pertinent communications available to Mr. Neuman's co-defendants was a basis for suppression. Indeed, Mr. Neuman had not yet filed his motion to suppress.

On September 8, 2011, Judge Johnson issued a protective order providing that the co-defendants must deliver to the Court, for placement under seal, Mr. Neuman's privileged and non-pertinent intercepted telephone calls and emails, and that the co-defendants must not disclose the content of these calls and emails. *See* Protective Order, September 8, 2011, Docket No. 54. Judge Johnson's protective order did not address whether the government's misconduct in making these privileged and non-pertinent communications available to the co-defendants was a basis for suppression.

* * *

Thus, in addition to the other bases for suppression set forth in Mr. Neuman's motion papers and articulated at oral argument, this Court should suppress the evidence obtained from the wiretap of Mr. Neuman's telephone and the search of his emails because the government wrongfully made available Mr. Neuman's privileged and non-pertinent calls and emails to the co-defendants in this case.

Respectfully submitted,

s/Susan R. Necheles
HAFETZ NECHELES & ROCCO
Susan R. Necheles
Joshua R. Geller
500 Fifth Avenue
29th Floor
New York, New York 10110
212-997-7595
snecheles@hnrlawoffices.com
jgeller@hnrlawoffices.com

Attorneys for Defendant Moses Neuman

cc: All Counsel (*via ECF*)